SLOVENSKI STANDARD
SIST EN 1300:2014

01-julij-2014

Nadomešča:

SIST EN 1300:2004+A1:2011

Varnostne shranjevalne enote - Klasifikacija visoko varnostnih ključavnic po odpornosti proti nepooblaščenemu odpiranju

Secure storage units - Classification for high security locks according to their resistance to unauthorized opening

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

Unités de stockage en lieux sûrs - Classification des serrures haute sécurité en fonction de leur résistance à l'éffraction

Ta slovenski standard je istoveten z: EN 1300:2013

ICS:

13.310	Varstvo pred kriminalom	Protection against crime
35.220.99	Druge naprave za shranjevanje podatkov	Other data storage devices

SIST EN 1300:2014 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 1300

November 2013

ICS 13.310

Supersedes EN 1300:2004+A1:2011

English Version

Secure storage units - Classification for high security locks according to their resistance to unauthorized opening

Unités de stockage en lieux sûrs - Classification des serrures haute sécurité en fonction de leur résistance à l'effraction

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

This European Standard was approved by CEN on 14 May 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword ...3
1 Scope ...6
2 Normative references ...6
3 Terms and definitions ...7
4 Classification ... 11
5 Requirements ... 11
6 Technical documentation ... 20
7 Test specimens ... 21
8 Test methods ... 22
9 Test report ... 31
10 Marking ... 32
Annex A (normative) Parameters for installation and operating instructions ... 33
Annex B (normative) Determination of manipulation resistance due to the design requirement ... 35
Annex C (normative) Manufacturer's Declaration (applies only to key operated locks) ... 42
Annex D (informative) Lock dimensions ... 43
Annex E (informative) A-deviations ... 44
Bibliography ... 46

Foreword

This document (EN 1300:2013) has been prepared by Technical Committee CEN/TC 263 “Secure storage of cash, valuables and data media”, the secretariat of which is held by BSI.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2014, and conflicting national standards shall be withdrawn at the latest by May 2014.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 1300:2004+A1:2011.

In comparison with EN 1300:2004+A1:2011, the following changes have been made:

- addition of definitions (Clause 3) and requirements (subclause 5.1.6) for contactless electronic tokens;
- addition of definitions (Clause 3) and requirements (subclause 5.1.7) for cryptography in distributed security systems;
- updating references to newer versions;
- changing of the requirements for the input unit (subclause 5.1.5.4);
- updating the test specimen of keys to a middle key cut design (subclause 7.3);
- clarification and optimization of the immersion test (subclause 8.2.6.3);
- correction of the heat resistance test (subclause 8.2.7.2);
- editorial clarifications among others in subclauses 5.1.5.1, 5.2.7, 5.3.3, 7.1, 8.2.2.1, 8.2.4.3.2, 8.2.6.2 and 8.3.3.3.2;
- addition of parameters for operating instructions in Annex A.

This document reflects the market demand to include requirements for distributed systems and electronic tokens and responds to the state of the art requirements when it was written down.

This European Standard has been prepared by Working Group 3 of CEN/TC 263 as one of a series of standards for secure storage of cash valuables and data media. Other standards in the series are, among others:

- EN 1047-1, *Secure storage units — Classification and methods of test for resistance to fire — Part 1: Data cabinets and diskette inserts*
- EN 1047-2, *Secure storage units — Classification and methods of test for resistance to fire — Part 2: Data rooms and data container*
- EN 1143-1, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Part 1: Safes, ATM safes, strongroom doors and strongrooms*

- EN 1143-2, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Part 2: Deposit systems*
- EN 14450, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Secure safe cabinets*

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

This European Standard also specifies requirements for high security electronic locks (HSL) which are controlled remotely. Regarding distributed systems, this standard responds to the state of the art requirements when it was written down. It is mandatory that the standard has to be revised with a frequency of 3 years as the research in the area of cryptography and relevant attacks evolve with high speed as well as the referenced standards.

1 Scope

This European Standard specifies requirements for high security locks (HSL) for reliability, resistance to burglary and unauthorized opening with methods of testing. It also provides a scheme for classifying HSL in accordance with their assessed resistance to burglary and unauthorized opening.

It applies to mechanical and electronic HSL. The following features may be included as optional subjects but they are not mandatory:

a) recognized code for preventing code altering and/or enabling/disabling parallel codes;

b) recognized code for disabling time set up;

c) integration of alarm components or functions;

d) remote control duties;

e) resistance to attacks with acids;

f) resistance to X-rays;

g) resistance to explosives;

h) time functions.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 1143-1, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Part 1: Safes, ATM safes, strongroom doors and strongrooms*

EN 60068-2-1:2007, *Environmental testing — Part 2-1: Tests — Test A: Cold (IEC 60068-2-1:2007)*

EN 60068-2-2:2007, *Environmental testing — Part 2-2: Tests — Test B: Dry heat (IEC 60068-2-2:2007)*

EN 60068-2-6:2008, *Environmental testing — Part 2-6: Tests — Test Fc: Vibration (sinusoidal) (IEC 60068-2-6:2007)*

EN 60068-2-17:1994, *Environmental testing — Part 2: Tests — Test Q: Sealing (IEC 60068-2-17:1994)*

EN 61000-4-2, *Electromagnetic compatibility (EMC) — Part 4-2: Testing and measurement techniques — Electrostatic discharge immunity test (IEC 61000-4-2)*

EN 61000-4-3, *Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques — Radiated, radio-frequency, electromagnetic field immunity test (IEC 61000-4-3)*

EN 61000-4-4, *Electromagnetic compatibility (EMC) — Part 4-4: Testing and measurement techniques — Electrical fast transient/burst immunity test (IEC 61000-4-4)*

EN 61000-4-5, *Electromagnetic compatibility (EMC) — Part 4-5: Testing and measurement techniques — Surge immunity test (IEC 61000-4-5)*

EN 61000-4-6, *Electromagnetic compatibility (EMC) — Part 4-6: Testing and measurement techniques — Immunity to conducted disturbances, induced by radio-frequency fields (IEC 61000-4-6)*

EN ISO 6988, *Metallic and other non-organic coatings — Sulfur dioxide test with general condensation of moisture (ISO 6988)*

ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 9798-2, *Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*

ISO/IEC 9798-4, *Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
High Security Lock
HSL
independent assembly normally fitted to doors of secure storage units

Note 1 to entry: Codes can be entered into an HSL for comparison with memorized codes (processing unit). A correct match of an opening code allows movement of a blocking feature.

3.2
code
identification information required which can be entered into a HSL and which, if correct, enables the security status of the HSL to be changed

3.2.1
opening code
identification information which allows the HSL to be opened

3.2.2
recognized code
identification information which allows access to the processing unit and which may also be an opening code

3.2.3
duress code
parallel code which initiates some additional function

3.2.4
parallel code
opening code which has identical function to that of an existing opening code but constructed of different figures

3.3
coding means
method by which the code is held

3.3.1
material code
code defined by the physical features or other properties of a token

3.3.2
mnemonic code
remembered code consisting of numeric and/or alphabetic information

3.3.3
biometric code
code comprising human characteristics

3.3.4
one time code
code changing after each use generated by use of an algorithm

3.4
input unit
part of an HSL which communicates codes to a processing_unit

3.5
processing unit
part of an HSL which evaluates whether the input code is correct and enables or prevents movement of a locking device

3.6
locking device
bolt stump or bolt stumps which form part of an HSL which enables or prevents movement of a blocking feature

3.7
token
object whose physical form or properties defines a recognized code, e.g. a key

Note 1 to entry: An electronic token incorporates an integrated circuit containing volatile and non-volatile memory, associated software and in many cases a microcontroller which communicates with an input unit by contact or contactless means.

3.8
mechanical HSL
HSL which is secured by means of mechanical elements only

3.9
electronic HSL
HSL which is secured partly or fully by electrical or electronic elements

3.10
blocking feature
part of a HSL which, after inputting the correct opening code moves, or can be moved

Note 1 to entry: A blocking feature either secures a door or prevents movement of a boltwork. The bolt of a mechanical lock is an example of a blocking feature.

3.11
destructive burglary
attack which damages the HSL in such a manner that it is irreversible and cannot be hidden from the authorized user

3.12
reliability
ability to function and achieve the security requirements of this standard after a large number of duty cycles

3.13
manipulation
method of attack aimed at removing the blocking function without causing damage obvious to the user

Note 1 to entry: A HSL may function after manipulation although its security could be permanently degraded.

3.14
spying
attempt to obtain unauthorized information

3.15
usable codes
codes or tokens permitted by the manufacturer and conforming to the requirements of this standard

Note 1 to entry: For mechanical HSL the number of usable codes is much less than the total number of codes to which the HSL can be set.

3.16
scrambled condition
coding elements are not in the configuration necessary for the HSL to be opened without entering the complete correct code or proper token

3.17
locking sequence
series of actions which start with an open door and are complete when the door is closed, bolted, locked and secure

3.18
open door
door is not in its frame

3.19
closed door
door is within its frame ready for throwing its bolt(s)

3.20
bolted door
bolts are thrown

3.21
locked door
boltwork cannot be withdrawn because of the HSL

3.22
secured door
door is closed, bolted and locked with an HSL in the secured HSL condition

3.23
secured HSL condition
blocking feature is thrown and can only be withdrawn after entering the opening code(s)

3.24
normal condition
after testing, the HSL specimen is in the secured HSL condition, and all design functions are operating

3.25
operating condition
after testing, the HSL specimen is in the secured HSL condition and can be unlocked with the opening code(s), but not all design functions are operable

3.26
fail secure
after testing, the HSL specimen is in the secured HSL condition, but not all design functions are operable therefore it cannot be unlocked with the opening code(s)

3.27
resistance unit
RU
value for burglary and manipulation resistance

Note 1 to entry: It shows a calculated result from using a tool with a certain value over a period of time.

3.28
penalty time
time delay because of time exceeding the limit of trials

3.29
authentication
method to prevent fraud by ensuring that communication with components of a distributed system can only be established after the identity of the components have been properly confirmed

3.30
cryptographic algorithm
mathematical method for the transformation of data that includes the definition of parameters (e.g. key length and number of iterations or rounds)

3.30.1
asymmetric cryptographic algorithm
cryptographic algorithm that uses two related keys, a public key and a private key, which have the property that deriving the private key from the public key is computationally infeasible

3.30.2
symmetric cryptographic algorithm
cryptographic algorithm that uses a single secret key for both encryption and decryption

3.31
cryptographic key
parameter used in conjunction with a cryptographic algorithm which is used to control a cryptographic process such as encryption, decryption or authentication

Note 1 to entry: Knowledge of an appropriate key allows correct en- and/or decryption or validation of a message.

3.32
cryptographic module
set of hardware and software that implements security functions for distributed systems and electronic tokens including cryptographic algorithms

3.33
distributed system
system with components connected by a transmission system, wired or wireless

Note 1 to entry: It is assumed that the transmitted information can be accessed by a third party. A high security lock with components in separate locations is defined as distributed system. A lock system with two input units, one on the safe and the other remote (= distributed input unit) is an example of a distributed system). An electronic lock with a non-accessible transmission system in the sense of 5.1.5.3 of this standard or with a temporary on-site wired connection to a mobile device (e.g. Personal Computer) supervised by an authorized person is not considered as a distributed system.

3.34
encryption
procedure that renders the contents of a message or file unintelligible to anyone not authorized to read it

Note 1 to entry: During the encryption procedure, a cryptographic algorithm using the cryptographic key is used to transform plaintext into cipher text. This procedure is composed of:

- the mode of operation, describing the way to process data with the algorithm;
- the padding scheme, describing the way to fill up data strings to a defined length.

3.35
transmission system
communication system between the elements of a distributed system

Note 1 to entry: Dedicated lines, wired and wireless public switched networks may be used as the transmission path.

3.36
security relevant information
codes according to 3.2, authentications, any code or key transmissions and changes as well as firmware updates of processing units

3.37
automatic key exchange
cryptographic protocol that allows two components that could have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel

3.38
availability
proportion of time a system is in functioning condition

4 Classification

HSL are classified to an HSL class (A, B, C or D) according to Table 1, Table 2 and Table 3 by their security requirements. General requirements (see 5.1 and 5.2, 5.3) security and reliability requirements shall be met.

NOTE HSL class A has the lowest requirements and HSL class D has the highest requirements.

5 Requirements

5.1 General requirements

All requirements shall be tested according to 8.1.2.

5.1.1 Requirements for all classes

5.1.1.1 HSL shall only be opened by valid opening codes. The opening code(s) shall be retained as the only valid opening code(s) until deliberately reset. Overlaying or undocumented code(s) are not permitted.

5.1.1.2 Where mnemonic codes are used with a HSL these shall be able to be changed.

5.1.1.3 Any supplementary device (e.g. micro switch) which is fitted by the HSL manufacturer shall not be capable of being used to obtain information about the code.

5.1.1.4 An input unit is a necessary part of a HSL although one input unit may operate more than one HSL (processing unit). Each HSL shall have a processing unit to validate the correct code from the input unit.